M·H

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	**WEITERES VORGEHEN**	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
PHD 99.096WO		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 99/07025	21/09/1999	30/09/1998
Anmelder		
KONINKLIJKE PHILIPS ELECTRONICS N.V. et al.		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [X] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [ ] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/07025

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06K19/073

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G06K G11C G06F G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 4 932 053 A (FRUHAUF SERGE ET AL) 5. Juni 1990 (1990-06-05) Zusammenfassung Spalte 2, Zeile 4 - Zeile 26 Spalte 3, Zeile 26 -Spalte 5, Zeile 38 Abbildung 1	1,2,4-7, 9,10
A	EP 0 482 975 A (GEMPLUS CARD INT) 29. April 1992 (1992-04-29) in der Anmeldung erwähnt Zusammenfassung Spalte 1, Zeile 1 -Spalte 2, Zeile 44 Abbildung 1	1,6,11
A	US 5 265 162 A (BUSH GEORGE ET AL) 23. November 1993 (1993-11-23) Zusammenfassung Spalte 1, Zeile 13 -Spalte 2, Zeile 60	1,6

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
5. Januar 2000	12/01/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Jacobs, P

INTERNATIONAL SEARCH REPORT

Inter. .onal Application No
PCT/EP 99/07025

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06K19/073

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06K G11C G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 June 1990 (1990-06-05) abstract column 2, line 4 - line 26 column 3, line 26 -column 5, line 38 figure 1	1,2,4-7, 9,10
A	EP 0 482 975 A (GEMPLUS CARD INT) 29 April 1992 (1992-04-29) cited in the application abstract column 1, line 1 -column 2, line 44 figure 1	1,6,11
A	US 5 265 162 A (BUSH GEORGE ET AL) 23 November 1993 (1993-11-23) abstract column 1, line 13 -column 2, line 60	1,6

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
5 January 2000	12/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Jacobs, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte...ional Application No
PCT/EP 99/07025

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4932053 A	05-06-1990	FR 2638869 A	11-05-1990
		EP 0368727 A	16-05-1990
		JP 2199561 A	07-08-1990
		JP 2813663 B	22-10-1998
EP 0482975 A	29-04-1992	FR 2667715 A	10-04-1992
		CA 2053001 A,C	10-04-1992
		DE 69100836 D	03-02-1994
		DE 69100836 T	09-06-1994
		ES 2065646 T	16-02-1995
		JP 4263384 A	18-09-1992
		US 5477039 A	19-12-1995
US 5265162 A	23-11-1993	US 5130519 A	14-07-1992

PCT WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : G06K 19/073 — A1

(11) Internationale Veröffentlichungsnummer: **WO 00/19367**

(43) Internationales Veröffentlichungsdatum: 6. April 2000 (06.04.00)

(21) Internationales Aktenzeichen: PCT/EP99/07025

(22) Internationales Anmeldedatum: 21. September 1999 (21.09.99)

(30) Prioritätsdaten:

198 44 962.3	30. September 1998 (30.09.98)	DE
199 36 938.0	5. August 1999 (05.08.99)	DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL–5621 BA Eindhoven (NL).

(71) Anmelder *(nur für DE)*: PHILIPS CORPORATE INTELLECTUAL PROPERTY GMBH [DE/DE]; Habsburgerallee 11, D–52066 Aachen (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: FEUSER, Markus [DE/NL]; Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(74) Anwalt: PETERS, Carl, H.; Internationaal Octrooibureau B.V., Prof. Holstlaan 6, NL–5656 AA Eindhoven (NL).

(81) Bestimmungsstaaten: JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

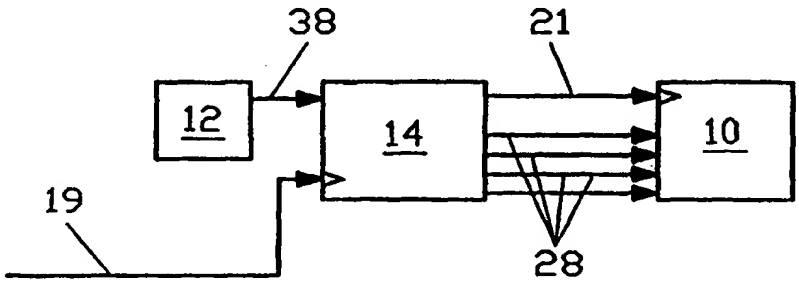
Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: DATA PROCESSING DEVICE AND OPERATING METHOD FOR PREVENTING A DIFFERENTIAL CURRENT CONSUMPTION ANALYSIS

(54) Bezeichnung: DATENVERARBEITUNGSEINRICHTUNG UND VERFAHREN ZU DESSEN BETRIEB ZUM VERHINDERN EINER DIFFERENTIELLEN STROMVERBRAUCHANALYSE

(57) Abstract

The invention relates to a data processing device (100) and to a method for operating a data processing device, notably a chip card. The device comprises an integrated circuit (10) which in accordance with a first clock pulse carries out useful calculations, notably cryptographic operations. To this end a second clock pulse is randomly derived from the first clock pulse and supplied to the integrated circuit (10) instead of the first clock pulse. Distances between the edges of the second clock pulse vary randomly over time. To this end the invention provides for a clock control unit (14) which is linked to the integrated circuit (10) as well as for a random generator (12) which is connected to the clock pulse control unit (14). The clock control unit (14) is configured such that it generates a second clock (20) in accordance with the random generator (12) and the first clock pulse (18), and the second clock pulse varies randomly and controls the integrated circuit (10).



(57) Zusammenfassung

Die vorliegende Erfindung betrifft eine Datenverarbeitungseinrichtung (100) sowie ein Verfahren zum Betreiben einer Datenverarbeitungseinrichtung, insbesondere einer Chipkarte, mit einer integrierten Schaltung (10), welche in Abhängigkeit von einem ersten Taktsignal Nutzrechenoperationen, insbesondere kryptographische Operationen, ausführt. Hierbei wird aus dem ersten Taktsignal zufallsgesteuert ein zweites Taktsignal abgeleitet und statt des ersten Taktsignals der integrierten Schaltung (10) zugeführt, wobei Abstände zwischen Taktflanken des zweiten Taktsignals zufällig über die Zeit variieren. Dazu ist eine mit der integrierten Schaltung (10) verbundene Taktsteuereinheit (14) sowie ein mit der Taktsteuereinheit (14) verbundener Zufallsgenerator (12) vorgesehen, wobei die Taktsteuereinheit (14) derart ausgebildet ist, dass sie in Abhängigkeit vom Zufallsgenerator (12) und dem ersten Taktsignal (18) ein zweites Taktsignal (20) erzeugt, welches zufällig variiert und die integrierte Schaltung (10) ansteuert.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien
AM	Armenien
AT	Österreich
AU	Australien
AZ	Aserbaidschan
BA	Bosnien-Herzegowina
BB	Barbados
BE	Belgien
BF	Burkina Faso
BG	Bulgarien
BJ	Benin
BR	Brasilien
BY	Belarus
CA	Kanada
CF	Zentralafrikanische Republik
CG	Kongo
CH	Schweiz
CI	Côte d'Ivoire
CM	Kamerun
CN	China
CU	Kuba
CZ	Tschechische Republik
DE	Deutschland
DK	Dänemark
EE	Estland
ES	Spanien
FI	Finnland
FR	Frankreich
GA	Gabun
GB	Vereinigtes Königreich
GE	Georgien
GH	Ghana
GN	Guinea
GR	Griechenland
HU	Ungarn
IE	Irland
IL	Israel
IS	Island
IT	Italien
JP	Japan
KE	Kenia
KG	Kirgisistan
KP	Demokratische Volksrepublik Korea
KR	Republik Korea
KZ	Kasachstan
LC	St. Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Litauen
LU	Luxemburg
LV	Lettland
MC	Monaco
MD	Republik Moldau
MG	Madagaskar
MK	Die ehemalige jugoslawische Republik Mazedonien
ML	Mali
MN	Mongolei
MR	Mauretanien
MW	Malawi
MX	Mexiko
NE	Niger
NL	Niederlande
NO	Norwegen
NZ	Neuseeland
PL	Polen
PT	Portugal
RO	Rumänien
RU	Russische Föderation
SD	Sudan
SE	Schweden
SG	Singapur
SI	Slowenien
SK	Slowakei
SN	Senegal
SZ	Swasiland
TD	Tschad
TG	Togo
TJ	Tadschikistan
TM	Turkmenistan
TR	Türkei
TT	Trinidad und Tobago
UA	Ukraine
UG	Uganda
US	Vereinigte Staaten von Amerika
UZ	Usbekistan
VN	Vietnam
YU	Jugoslawien
ZW	Zimbabwe

Datenverarbeitungseinrichtung und Verfahren zu dessen Betrieb zum Verhindern einer differentiellen Stromverbrauchanalyse.

Die Erfindung betrifft ein Verfahren zum Betreiben einer Datenverarbeitungseinrichtung, insbesondere einer Chipkarte, mit einer integrierten Schaltung, welche in Abhängigkeit von einem ersten Taktsignal Nutzrechenoperationen, insbesondere kryptographische Operationen, ausführt, gemäß dem Oberbegriff des Anspruchs 1. Die Erfindung betrifft ferner eine Datenverarbeitungseinrichtung, insbesondere Chipkarte, insbesondere zum Ausführen des Verfahrens, mit einer integrierten Schaltung, welche in Abhängigkeit von einem ersten Taktsignal Nutzrechenoperationen, insbesondere kryptographische Operationen, ausführt, gemäß dem Oberbegriff des Anspruchs 6.

In vielen Datenverarbeitungsgeräten mit integrierter Schaltung dienen beispielsweise kryptographische Operationen zum Schutz des Betriebes dieser Geräte bzw. zum Schutz von in dem Gerät transportierten Daten. Die hierfür notwendigen Rechenoperationen werden dabei sowohl von Standard-Rechenwerken als auch von dedizierten Crypto-Rechenwerken durchgeführt. Ein typisches Beispiel für letzteres sind Chipkarten bzw. IC-Karten. Bei in diesem Zusammenhang verwendeten Daten bzw. Zwischenergebnissen handelt es sich üblicherweise um sicherheitsrelevante Informationen, wie beispielsweise kryptographische Schlüssel oder Operanden.

Bei von der integrierten Schaltung durchgeführten Rechenoperationen, beispielsweise zur Berechnung von kryptographischen Algorithmen, werden logische Verknüpfungen zwischen Operanden bzw. Zwischenergebnissen durchgeführt. In Abhängigkeit von der verwendeten Technologie führen diese Operationen, insbesondere das Laden von leeren oder zuvor gelöschten Speicherbereichen bzw. Register mit Daten, zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei komplementärer Logik, wie beispielsweise der CMOS-Technik, tritt ein erhöhter Stromverbrauch dann auf, wenn der Wert einer Bit-Speicherzelle geändert wird, d.h. sein Wert sich von "0" auf "1" bzw. von "1" auf "0" ändert. Der erhöhte Verbrauch hängt dabei von der Anzahl der im Speicher bzw. Register geänderten Bitstellen ab. Mit anderen Worten lässt das Laden eines zuvor gelöschten Registers

einen Stromverbrauch proportional zum Hamminggewicht des in das leere Register geschriebenen Operanden (=Anzahl der Bits mit dem Wert "1") ansteigen. Durch eine entsprechende Analyse dieser Stromänderung könnte es möglich sein, Informationen über die berechneten Operationen zu extrahieren, so dass eine erfolgreiche Kryptoanalyse von geheimen Operanden, wie beispielsweise kryptographischen Schlüsseln, möglich ist. Mittels Durchführung mehrerer Strommessungen am Datenverarbeitungsgerät könnten beispielsweise bei sehr kleinen Signaländerungen eine hinreichende Extraktion der Informationen ermöglicht werden. Andererseits könnten mehrere Strommessungen eine ggf. erforderliche Differenzbildung ermöglichen. Diese Art der Kryptoanalyse wird auch als "Differential Power Analysis" bezeichnet, mittels derer ein Außenstehender durch reine Beobachtung von Änderungen des Stromverbrauches des Datenverarbeitungsgerätes eine ggf. unberechtigte Kryptoanalyse der kryptographischen Operationen, Algorithmen, Operanden bzw. Daten erfolgreich ausführen kann. Die "Differential Power Analysis" ermöglicht somit über eine reine Funktionalität hinaus zusätzliche interne Informationen einer integrierten Schaltung gewinnen zu können.

Aus der US 4 813 024 ist eine integrierte Schaltung zum Speichern und Verarbeiten geheimer Daten bekannt, wobei ein Speicher eine Simulationsspeicherzelle aufweist, welche einen identischen Stromverbrauch aufweist wie eine Speicherzelle, die bisher nicht programmiert wurde. Hierdurch werden Schwankungen in Strom und Spannung größtenteils aber nicht ganz eliminiert. Dieses System ist auch aufwendig und kostenintensiv.

Bei einer aus der EP 0 482 975 B1 bekannten Speicherkarte mit Mikroschaltung und wenigstens einem Speicher, die an einem Datenverarbeitungsorgan angeschlossen ist, wobei das Datenverarbeitungsorgan von einem Datensignal von außerhalb der Karte gesteuert wird und als Antwort auf dieses Datensignal zu einem Zeitpunkt ein Befehlsendesignal abgibt, welches um eine vorbestimmte Dauer (T) bzgl. des Empfangs des Datensignals verzögert ist, wird zum Erhöhen des Schutzes die Zeitdauer (T) auf Zufallsbasis zeitlich variabel gewählt. Auf diese Weise unterliegt eine Zeitspanne zwischen einem Empfang eines externen Signals und einer Anwort einem Zufallsgenerator und ist nicht zur Auswertung zum Erhalten von geheimen Daten geeignet. Eine Kryptoanalyse auf der Basis einer Stromänderung beim Beschreiben des Speichers bzw. bei Durchführen von Rechenoperationen kann dieses System jedoch nicht verhindern.

Aus der EP 0 507 669 A1 ist es bei einer Karte für elektronische Zahlung, einer sogen. Paycard, bekannt, jede Bezahleinheit nicht mit einem einzigen Bit sondern mit mehreren Bits zu besetzen, wobei die zusätzlichen Bits in einer Zufallsreihe die

Bezahleinheiten durchnumerieren und von einer Zufallszahlenreihe abgeleitet sind. Diese Zufallszahlenreihe steht Verkäufern, welche eine Paycard akzeptieren, zur Verfügung. Auch dieses System kann jedoch eine Kryptoanalyse auf der Basis einer Stromänderung beim Beschreiben des Speichers bzw. bei Durchführen von Rechenoperationen nicht verhindern.

Die FR 2 693 014 B1 beschreibt eine Vorrichtung zum Auswerten von Chipkarten, wie beispielsweise eine öffentliche Telefonzelle, welche mittels einer Kapazitätsmessung feststellt, ob an eine eingeschobene Chipkarte externe Geräte angeschlossen sind.

Es ist Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren und eine verbesserte Datenverarbeitungseinrichtung der obengenannten Art zur Verfügung zu stellen, welche die obengenannten Nachteile beseitigen und einen wirksamen Schutz gegen eine "Differential Power Analysis" zur Verfügung stellen.

Diese Aufgabe wird durch ein Verfahren der o.g. Art mit den in Anspruch 1 gekennzeichneten Merkmalen und durch eine Datenverarbeitungseinrichtung der o.g. Art mit den in Anspruch 6 gekennzeichneten Merkmalen gelöst.

Dazu ist es bei dem Verfahren der o.g. Art erfindungsgemäß vorgesehen, dass aus dem ersten Taktsignal zufallsgesteuert ein zweites Taktsignal abgeleitet und statt des ersten Taktsignals der integrierten Schaltung zugeführt wird, wobei Abstände zwischen Taktflanken des zweiten Taktsignals zufällig über die Zeit variieren.

Dies hat den Vorteil, dass ein zeitlicher Ablauf von Nutzrechenoperationen unabhängig von in der Datenverarbeitungseinrichtung bearbeiteten Daten verzerrt wird, so dass ein bzgl. der Nutzrechenoperationen charakteristischer Anteil in einem Stromverbrauch der integrierten Schaltung verschleiert wird und mittels einer "Differential Power Analysis" nicht mehr analysierbar ist.

Vorzugsweise Weitergestaltungen des Verfahrens sind in den Ansprüchen 2 bis 5 beschrieben.

Zur weiteren Verschleierung eines charakteristischen Anteiles im Stromverbrauch der integrierten Schaltung von Berechnung bzw. Nutzoperationen der integrierten Schaltung wird die integrierte Schaltung zufallsgesteuert in verschiedene Betriebsarten geschaltet.

Zum Verhindern einer Wiederholbarkeit des charakteristischen Anteils im Stromverbrauch von identischen Nutzoperationen umfassen die verschiedenen Betriebsarten

wenigstens zwei Berechnungsmethoden, welche auf verschiedenen Berechnungswegen ein identisches Ergebnis erhalten.

Zur weiteren Verschleierung von Art und Zeitpunkt der Nutzrechenoperationen umfassen die verschiedenen Betriebsarten wenigstens eine Betriebsart "Dummy", bei der von der integrierten Schaltung keine Nutzoperationen sondern Dummyrechenoperationen durchgeführt werden, welche vorbestimmte oder zufällig gewählte Eingangsdaten bearbeiten, wobei das Ergebnis verworfen wird und nicht in die Ergebnisse bzw. Eingangsdaten der Nutzrechenoperationen eingehen. Optional ist zusätzlich eine Betriebsart "Deaktiviert" vorgesehen, bei der von der integrierten Schaltung keine Rechenoperationen ausgeführt werden.

Bei einer Datenverarbeitungseinrichtung der o.g. Art ist es erfindungsgemäß vorgesehen, dass eine mit der integrierten Schaltung verbundene Taktsteuereinheit sowie ein mit der Taktsteuereinheit verbundener Zufallsgenerator vorgesehen ist, wobei die Taktsteuereinheit derart ausgebildet ist, dass sie in Abhängigkeit vom Zufallsgenerator und dem ersten Taktsignal ein zweites Taktsignal erzeugt, welches zufällig variiert und die integrierte Schaltung ansteuert.

Dies hat den Vorteil, dass ein zeitlicher Ablauf von Nutzrechenoperationen unabhängig von in der Datenverarbeitungseinrichtung bearbeiteten Daten verzerrt wird, so dass ein bzgl. der Nutzrechenoperationen charakteristischer Anteil in einem Stromverbrauch der integrierten Schaltung verschleiert wird und mittels einer "Differential Power Analysis" nicht mehr analysierbar ist.

Vorzugsweise Weitergestaltungen der Datenverarbeitungseinrichtung sind in den Ansprüchen 7 bis 10 beschrieben.

Nachstehend wird die Erfindung anhand der beigefügten Zeichnungen näher erläutert. Diese zeigen in

Fig. 1 ein Blockschaltbild einer bevorzugte Ausführungsform einer erfindungsgemäßen Datenverarbeitungseinrichtung und

Fig. 2 eine graphische Veranschaulichung verschiedener in der Datenverarbeitungseinrichtung erzeugter und verwendeter Signale.

Fig. 1 zeigt eine bevorzugte Ausführungsform einer erfindungsgemäßen Datenverarbeitungseinrichtung 100 mit einer integrierten Schaltung 10, einem Zufallsgenerator 12 und einer Taktsteuereinheit 14. Die integrierten Schaltung 10 führt nachfolgend näher spezifizierte Nutzrechenoperationen aus. Nutzrechenoperationen sind solche Rechenoperationen, welche Eingangsdaten in gewünschter Weise bearbeiten und ein gewünschtes Ergebnis bzw. Zwischenergebnis erzielen. Ein Beispiel hierfür ist eine vorbestimmte Rechenmethode mit kryptographischen Operationen in dedizierten Crypto-Rechenwerken. Diese vorbestimmte Rechenmethode wird nachfolgend als Methode 1 bzw. erste Betriebsart bezeichnet.

Fig. 2 veranschaulicht übereinander verschiedene in der Datenverarbeitungseinrichtung 100 erzeugte und verwendete Signale über die Zeit t, welche über einer horizontalen Achse 16 aufgetragen sind 18 ist ein Signal $TAKT_1$, welches über eine Leitung 19 die Taktsteuereinheit 14 steuert. Mit 20 ist ein Signal $TAKT_2$ bezeichnet, welches von der Taktsteuereinheit 14 erzeugt und über eine Leitung 21 an die integrierte Schaltung 10 ausgegeben wird. 22 ist ein Signal DUMMY, mit 24 ein Signal DEAKT und mit 26 ist ein Signal ALT bezeichnet, welche über Steuerleitungen 28 von der Taktsteuereinheit 14 an die integrierte Schaltung 10 zum Steuern derselben abgegeben werden. In einer zusätzlichen Zeile 29 ist angegeben, in welcher Betriebsart die integrierte Schaltung 10 gesteuert von der Taktsteuereinheit 14 gerade arbeitet. Hierbei steht 30 für eine Betriebsart "Methode 1", 32 für eine Betriebsart "Dummy", 34 für eine Betriebsart "Methode 2" und 36 für eine Betriebsart "Deaktiviert". Nachfolgend werden diese Betriebsarten 30, 32, 34 und 36 und ihre Funktion näher erläutert.

Eine von Paul Kocher im Internet unter http://www.cryptography.com/dpa veröffentlichte "Differential Power Analysis" hat den Ansatz, dass neben den Ein/Ausgangssignalen zusätzlich eine Stromaufnahme I_a bzw. Spannungseinbrüche ΔU_a einer Versorgungsspannung U_a der integrierten Schaltung analysiert werden. Der Erfolg dieser Analysemethode hängt davon ab, ob man eine Anzahl N_A von analogen ($I_a(t)$ oder $\Delta U_a(t)$) Signalverläufen S(k,t) über die Zeit mit $k=\{1,...N_A\}$ unterschiedlichen Operanden derart aufnehmen kann, dass eine Summenbildung der Form

$$T(i,t) = \sum_{k=1}^{N_A} p(i,k) \cdot S(k,t)$$

mit den Koeffizienten p(i,k) mit $i=\{0,1,2,...\}$ möglich ist. Betrachtet man unterschiedliche Signalverläufe $S(k_1,t_1)$, $S(k_2,t_1)$, $S(k_3,t_1)$... zum gleichen Zeitpunkt $t=t_1$, kann eine "Differential

Power Analysis" nur funktionieren, wenn die integrierte Schaltung in diesem Moment die gleiche Rechenoperation mit unterschiedlichen Operanden $k=\{1,...,N_A\}$ ausführt, d.h. die Signalverläufe S(k,t) müssen genau übereinandergelegt werden können. Dieses gilt nicht nur für die Berechnung selbst, sondern auch für die Ein- und Ausgabe von Daten.

Die Erfindung verhindert das "Übereinanderlegen", indem die integrierte Schaltung 10 durch die zufallsgesteuerte Taktsteuereinheit 14 betrieben wird. Darüber hinaus verfügt die integrierte Schaltung neben der Betriebsart "Methode 1" 30 über die Betriebsart "Dummy" 32, in der nachfolgend näher spezifizierte Dummyrechenoperationen ausgeführt werden, die Betriebsart "Deaktiviert" 36, in der von der integrierten Schaltung 10 keine Rechenoperationen ausgeführt und bisherige Resultate bzw. Zwischenergebnisse ggf. gespeichert werden, und die Betriebsart "Methode 2" 34, in der die Nutzrechenoperationen von "Methode 1" 30 mit einem alternativen Verfahren ausgeführt werden, wobei sich das Ergebnis nicht von der ersten Betriebsart "Methode 1" 30 unterscheidet sondern lediglich anders gerechnet wird, so dass sich bei "Methode 2" 34 im Vergleich mit "Methode 1" 30 ein anderer Verlauf des Eingangsstromes I_a bzw. von Spannungsänderungen ΔU_a der integrierten Schaltung 10 bei gleichem Operanden k ergibt.

Dummyrechenoperationen sind solche Rechenoperationen, welche vorbestimmte oder zufällig gewählte Eingangsdaten bearbeiten, wobei das Ergebnis verworfen wird und nicht in die Ergebnisse bzw. Eingangsdaten der Nutzrechenoperationen eingehen.

Die Taktsteuereinheit 14 wird über Leitung 19 durch das Signal $TAKT_1$ 18 sowie von dem Zufallsgenerator 12 über Leitung 38 gesteuert. Die Taktsteuereinheit 14 generiert aus $TAKT_1$ 18 und dem Eingang von Leitung 38 ein zufälliges Taktsignal $TAKT_2$ 20, welches die Zeitachse 16 in S(k,t) unabhängig von in der integrierten Schaltung 10 gerechneten Daten verzerrt. Hierdurch ist die o.g. Summenbildung der "Differential Power Analysis" nicht mehr mit dem gewünschten Ergebnis durchführbar.

Ferner werden von einer Taktflanke bis zu einer später folgenden Taktflanke auf die Steuerleitungen 28 in Abhängigkeit vom Zufallsgenerator die Steuersignale DUMMY 22, DEAKT 24 und ALT 26 in der in Fig. 2 dargestellten Weise gesetzt. Bei dem Signal DUMMY 22 befindet sich die integrierte Schaltung 10 in der Betriebsart "Dummy" 32, bei dem Signal DEAKT 24 befindet sich die integrierte Schaltung 10 in der Betriebsart Deaktiviert 36, bei dem Signal ALT 26 befindet sich die integrierte Schaltung 10 in der Betriebsart "Methode 2" 34 und bei keinem Signal auf den Steuerleitungen 28 befindet sich die integrierte Schaltung 10 in der Betriebsart "Methode 1" 30, wie aus der die Betriebsarten angebenden Zeile 29 in Fig. 2 ersichtlich.

Die Betriebsart "Dummy" 32 verschleiert die eigentliche Berechnung S(k,t). Ggf. sind mehrere verschiedene Betriebsarten "Dummy n" mit entsprechenden verschiedenen Signalen "DUMMY n" vorgesehen. Besonders vorteilhaft ist hier, dass Zeitpunkt und Dauer der Dummysignale nicht von der zu schützenden integrierten Schaltung 10 selbst sondern durch die externen Einrichtungen Zufallsgenerator 12 und Taktsteuereinheit 14 bestimmt werden. In der Betriebsart "Deaktiviert" 36 wird die Zeitachse 16 weiter zusätzlich verzerrt, so dass die o.g. Summenbildung der "Differential Power Analysis" zusätzlich erschwert bzw. unmöglich wird. In der Betriebsart "Methode 2" 34 erfolgt eine weitere Verschleierung der Berechnung, so dass die Berechnung S(k,t) schlecht identifizierbar ist. Ggf. sind weitere unterschiedliche Betriebsarten mit anderem Berechnungsweg "Methode n" vorgesehen, jeweils zugehörigen Signalen "ALT n".

Zusammenfassend wird erfindungsgemäß ein charakteristischer Anteil des Stromverbrauchs der integrierten Schaltung 10 nicht eliminiert sondern verschleiert. Hierzu werden flexibel verschiedene Verschleierungsmethoden mittels der Taktsteuereinheit 14 miteinander kombiniert. Teilweise werden durch Dummyberechnungen Dummysignale generiert, welche von außen als solche nicht erkennbar sind, da sie zufällig erzeugt werden.

BEZUGSZEICHENLISTE:

100	Datenverarbeitungseinrichtung
10	integrierte Schaltung
12	Zufallsgenerator
14	Taktsteuereinheit
16	horizontalen Achse t
18	Signal $TAKT_1$
19	Leitung
20	Signal $TAKT_2$
21	Leitung
22	Signal DUMMY
24	Signal DEAKT
26	Signal ALT
28	Steuerleitungen
29	Zeile Betriebsarten
30	Betriebsart "Methode 1"
32	Betriebsart "Dummy"
34	Betriebsart "Methode 2"
36	Betriebsart "Deaktiviert"
38	Leitung

PATENTANSPRÜCHE:

1. Verfahren zum Betreiben einer Datenverarbeitungseinrichtung (100), insbesondere einer Chipkarte, mit einer integrierten Schaltung (10), welche in Abhängigkeit von einem ersten Taktsignal Nutzrechenoperationen, insbesondere kryptographische Operationen, ausführt, dadurch gekennzeichnet, dass aus dem ersten Taktsignal zufallsgesteuert ein zweites Taktsignal abgeleitet und statt des ersten Taktsignals der integrierten Schaltung (10) zugeführt wird, wobei Abstände zwischen Taktflanken des zweiten Taktsignals zufällig über die Zeit variieren.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die integrierte Schaltung (10) zufallsgesteuert in verschiedene Betriebsarten geschaltet wird.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass die verschiedenen Betriebsarten wenigstens zwei Berechnungsmethoden umfassen, welche auf verschiedenen Berechnungswegen ein identisches Ergebnis erhalten.

4. Verfahren nach einem der Ansprüche 2 oder 3, dadurch gekennzeichnet, dass die verschiedenen Betriebsarten wenigstens eine Betriebsart "Dummy" (32) umfassen, bei der von der integrierten Schaltung (10) keine Nutzoperationen sondern Dummyrechenoperationen durchgeführt werden, welche vorbestimmte oder zufällig gewählte Eingangsdaten bearbeiten, wobei das Ergebnis verworfen wird und nicht in die Ergebnisse bzw. Eingangsdaten der Nutzrechenoperationen eingehen.

5. Verfahren nach einem der Ansprüche 2 bis 4, dadurch gekennzeichnet, dass die verschiedenen Betriebsarten eine Betriebsart "Deaktiviert" (36) umfassen, bei der von der integrierten Schaltung (10) keine Rechenoperationen ausgeführt werden.

6. Datenverarbeitungseinrichtung (100), insbesondere Chipkarte, insbesondere zum Ausführen eines Verfahrens gemäß wenigstens einem der vorhergehenden Ansprüche, mit einer integrierten Schaltung (10), welche in Abhängigkeit von einem ersten Taktsignal

(18) Nutzrechenoperationen, insbesondere kryptographische Operationen, ausführt, dadurch gekennzeichnet, dass eine mit der integrierten Schaltung (10) verbundene Taktsteuereinheit (14) sowie ein mit der Taktsteuereinheit (14) verbundener Zufallsgenerator (12) vorgesehen ist, wobei die Taktsteuereinheit (14) derart ausgebildet ist, dass sie in Abhängigkeit vom Zufallsgenerator (12) und dem ersten Taktsignal (18) ein zweites Taktsignal (20) erzeugt, welches zufällig variiert und die integrierte Schaltung (10) ansteuert.

7. Datenverarbeitungseinrichtung (100) nach Anspruch 6, dadurch gekennzeichnet, dass die Taktsteuereinheit (14) derart ausgebildet ist, dass sie in Abhängigkeit vom Zufallsgenerator (12) die integrierte Schaltung (10) über Steuerleitungen (28) zufallsgesteuert in verschiedene Betriebsarten (30, 32, 34, 36) schaltet.

8. Datenverarbeitungseinrichtung (100) nach Anspruch 7, dadurch gekennzeichnet, dass die verschiedenen Betriebsarten (30, 32, 34, 36) wenigstens zwei Berechnungsmethoden (30, 34) umfassen, welche auf verschiedenen Berechnungswegen ein identisches Ergebnis erhalten.

9. Datenverarbeitungseinrichtung (100) nach einem der Ansprüche 7 oder 8, dadurch gekennzeichnet, dass die verschiedenen Betriebsarten (30, 32, 34, 36) wenigstens eine Betriebsart "Dummy" (32) umfassen, bei der die integrierte Schaltung (10) keine Nutzoperationen sondern Dummyrechenoperationen durchführt, welche vorbestimmte oder zufällig gewählte Eingangsdaten bearbeiten, wobei das Ergebnis nicht in Ergebnisse bzw. Eingangsdaten der Nutzrechenoperationen eingehen.

10. Datenverarbeitungseinrichtung (100) nach einem der Ansprüche 7 bis 9, dadurch gekennzeichnet, dass die verschiedenen Betriebsarten (30, 32, 34, 36) eine Betriebsart "Deaktiviert" (36) umfassen, bei der die integrierten Schaltung (10) keine Rechenoperationen ausführt.

11. Datenverarbeitungseinrichtung (100) nach einem der Ansprüche 7 bis 10, dadurch gekennzeichnet, dass mindestens bei einer weiteren Betriebsart die Zeitachse (16) weiter zusätzlich verzerrt wird, so dass die Summenbildung der „Differential Power Analysis“ zusätzlich erschwert bzw. unmöglich wird.

Fig.1

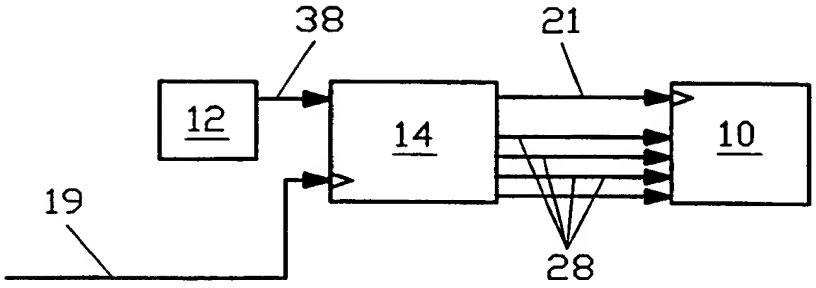


Fig.2